Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1747 12/18/15

~ Firebee Update News! ~ People Are Talking! ~ 2015 Game of the Year!
~ Real-name Policy Eased ~ Teen Secret Hashtags! ~ Konami/Kojima Spat!
~ Commander Keen Is 25! ~ Linear Classic Icons! ~ N3XT - 1000X Faster?

~ Trump Site Is Attacked ~ Sanitize Your Year! ~ Real Star Raiders II!

-* Government Hacking Twitter? *-
-* Lizard Squad's Christmas Eve Threat *-
-* Email Privacy Protected by 4th Amendment! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, it's nice to know that there are still quite a few out there who continue to read A-ONE regularly. I base that statement on the few e-mails that I received over the past two weeks because of some of my editorial comments. The purpose of editorial commentary, although severely lacking on my part for quite some time, is to invoke reflection of certain topics - both positive and negative.

My recent feedback references my comments regarding President Obama's initial speech after the terrorist attack in California. I also mentioned that Donald Trump should get some "credit" for having the testicular fortitude to speak his mind - whether you like him or not. While one reader appeared to agree with my position, a couple of our readers thought quite the opposite. For the record, I'm middle-of-the-road as far as Trump goes. There are things about him that I don't agree. There are times that I wished he stated views in a different manner. There are things about him that I do like, including his willingness to be open rather than dancing around the issues like most politicians tend to do in an effort to not offend anyone.

Anyway, just to refresh our readers' minds, here's what I wrote last week:

There's a reason why I despise talking religion and politics, and a bigger one as to discussing a combination of the two!! Everyone has his own opinion, and neither is necessarily wrong.

Last week, I briefly mentioned Obama's lame speech from the Oval Office with regard to the terrorist attack in California. All that came out of his mouth was pure BS. One came away from listening to him, and scratching your head with the conclusion of "what was all that about?" Just more of the same Obama rhetoric that we've been listening to for years.

Love him or hate him, right or wrong - you have to give Donald Trump some credit for having the cajones to speak his mind. I don't agree with everything that he has to say, but it's obvious that he's not pussy-footing around. Forget political-correctness for the moment - there are a number of major issues in today's world that need attention. Toes are going to get stepped on. Some people's feelings are going to get hurt. Things are still interesting in the world of politics!

Look at the slate of presidential candidates - from both parties. It's embarrassing! As one of my e-mails mentioned, the Republican candidates are spending more time answering questions about Trump than talking about the issues. He's right, they do. Instead of spending all this time trying to "knock down" the front-runner (amazing that Trump has been leading the polls since the beginning!), focus on individual campaigns and the issues! Let Trump either self-implode (if that's his inevitable fate) of let him prove himself a viable candidate. That's what they all should do.

Unfortunately, the focus at-hand is terrorism and what to do about it. As Dorothy said in The Wizard of Oz: "Toto, I don't think we're in Kansas any more!" No, Dorothy, we're not! The U.S. is no longer in its own seemingly protected part of the world. September 11, 2001 should have brought that fact to light. Move ahead to the present - the Russian passenger plane brought down over Egypt. The attacks in Paris. The attack in San Bernardino.

The world is not fighting a "conventional" war here; we're fighting what seems to be radical religious zealouts who have no regard for innocent human lives. They're aptly called terrorists. The world is not safe any more - these recent three terrorist attacks have shown that to be true.

Maybe it's time for more presidential candidates to start thinking in a more non-conventional manner rather than the same old, worn out rhetoric.

Until next time...

=~=~=~=

FireBee Update News

By Fred Horvat

Well I am finally back working with my FireBee again. Where I left off was updating my Firmware and TOS's to try and get certain supported software (Netsurf 3.4 and EasyMiNT) to run on my FireBee. I did all the updates and it appeared to install all fine but I still could not run that software. It was suggested on the FireBee Section on Atari-Forum http://www.atari-forum.com/viewtopic.php?f=92&t=28704 to inspect my DIP-Switch settings.

I looked on the Basic Information Sheet for the DIP-Switch settings and here is what was on the sheet:

DIP Switches and TOS Versions
DIP-switch are following from left
to right. Up indicates an On position.
1: write protect flash ON/OFF

2: CF-Socket is master drive ON/OFF
3-4: Go to PIC (currently unsupported)
5-6: FireTOS/EmuTOS selector
5 ON, 6 ON;
Run FireTOS without sound support
5 OFF, 6 ON;
Run EmuTOS in fully ColdFire native mode
Please note: EmuTOS or FireTOS usage has to be selected via DIPSwitches.
EmuTOS usage via FireTOS boot menu does not work as of yet.

When I looked for the switches it took me a minute or two to find them on the board. Once I did it was one of the rare times I was forced to wear my glasses as the switches are very small. For those who wish to follow at home my setting are:

1 : Off
2 : On
3 : Off
4 : Off
5 : On
6 : On

I posted my findings to the thread listed above but shortly before I submitted this installment so I will work with the feedback this coming week and work with the FireBee some more. Until next time.

Linear Classic Icons Set for Teradesk

The Linear Classic is a new 48pts RSC icons set for the Teradesk desktop. This set is a member of the Linear icons family but, while it adopts most of the pictograms from the Linear Blue set, it has different basic shapes for files, folders and programs, to improve users' interaction.

The Linear Classic set is composed by 206 icons drawn in 256, 16 and 2 colors, in the usual RSC(AES-4) format. A configuration file (teradesk.inf), optimised for the Official FireBee setup, is also included. If you already have a well customised Teradesk desktop with the Linear Blue 48pts set vers. 1.2 to 1.4b (The Linear Blue set was recently updated and is available in the support/look & feel section of firebee.org), you are only required to replace the cicons.rsc file as the teradesk.inf configuration files are upward compatible. To help users customise ther working spaces, several unassigned folder icons (folder1-folder7) were also included.

=~=~=~=

->In This Week's Gaming Section - Game of the Year: The Witcher 3: Wild Hunt!
Xbox Live Downed After Threats!
Hacker Confirms PlayStation 4 Jailbreak!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""""

Game of the Year: The Witcher 3: Wild Hunt

Video games officially leveled up in 2015. After a few dodgy transitional years there, the new consoles are finally delivering. PC gaming is thriving, and that phone in your pocket is a viable game machine. When it comes to both quantity and quality, 2015 was simply one of the best years on record.

That made picking our favorite a real nightmare, but eventually, a white-haired, demon-hunting warrior sliced through the contenders to give The Witcher 3: Wild Hunt our top honor.

A sprawling, open-world fantasy adventure fused with a tight, compelling narrative, The Witcher 3 is simultaneously epic and intimate, a truly impressive feat for a huge role-playing game. We burned countless hours searching for our protØgØ Ciri, battling massive beasts, playing the clever card game Gwent, and exploring every nook and cranny of developer CD Projekt Red s gorgeous, glorious world. Suffice to say, it was time well spent.

Tapped as a Game of the Year contender the moment it was unveiled at the E3 conference in June, Fallout 4 had a lot to live up to. And while it came up a bit short of our admittedly overblown expectations, Bethesda s post-apocalyptic RPG is still an amazing journey through a hand-crafted wasteland bursting with enemies to fight, locations to explore, and duct tape to pilfer. More addictive than Psycho-Jet, this one.

Bigger isn t always better, however. Wedged between these two open-world behemoths stands a game smaller of stature but equally compelling: Rocket League, the spectacular sleeper hit of 2015. Car soccer? Really? Spend more than a half-hour playing and it will hit you like a fender to the mouth. Easy to learn but tough to master, Rocket League s simple design belies its best-in-class performance. This was THE multiplayer game of 2015, and easily the game we logged the most time with.

More like what isn t. While 2015 was jam-packed with killer games, it s just the start of what s shaping up to be a new Golden Age for gamers. A wealth of incredibly cool games are lining up to take over our lives next year, including the impossibly big space game No Man s Sky, the breathtaking Uncharted 4, Microsoft s time-bending Quantum Break, the sequel to 2012 Game of the Year contender Dishonored, and the long-awaited Legend of Zelda game for the Wii U. Rest those thumbs you re gonna need em.

Next Xbox One Backward-compatible Games Revealed

After teasing that the next batch of Xbox One backward-compatible games would be announced "very soon," Microsoft has now followed through on that promise. The company today unveiled 16 new Xbox 360 games that are now playable on Xbox One through the feature. Scroll down below the image to see all of the games, but spoiler alert: Red Dead Redemption is sadly not one of them.

Xbox One Backward Compatibility Games Added December 17:

- Braid
- Deus Ex: Human Revolution
- Doritos Crash Course
- Fable III
- Halo: Reach
- Hydro Thunder
- Iron Brigade
- Kane & Lynch 2
- Motocross Madness
- Ms. Pac Man
- Peggle
- Portal: Still Alive
- Spelunky
- Splosion Man
- Ticket to Ride
- Zuma’s Revenge

November’s New Xbox One Experience update introduced backwards compatibility support (and lots of other new features) with an initial lineup of 104 games. Microsoft has pledged to release new games to the lineup on a regular basis. In addition to the games announced today, we’re expecting more next year.

In past interviews, Microsoft management has said backward compatibility should help boost Xbox One console sales, though what effect the feature has had in this department remains to be seen.

Microsoft also announced today that, since backward compatibility support arrived on November 12, people have logged more than 9 million hours playing Xbox 360 games on Xbox One. The most popular backward compatibility games, so far at least, are Fallout 3, Gears of War 3, Just Cause 2, Assassin’s Creed II, and Dirt 3.

With close to 130,000 votes, Call of Duty: Black Ops II is the most-requested Xbox 360 games for Xbox One backward compatibility on the Xbox Feedback website. Rounding out the top five are The Elder Scrolls V: Skyrim, Red Dead Redemption, Call of Duty: Modern Warfare 2, and Halo: Reach (a Microsoft game). With the exception of Halo: Reach, Microsoft has not yet delivered the other top-requested games.

There is no guarantee that Microsoft ever will, either, as whether or not games are added to the backward compatibility lineup is decided by individual publishers. Back in November,

Microsoft said it is holding discussions with all major publishers and developers, including Rockstar Games.

Games announced for Xbox One backward compatibility but not yet delivered include Halo Wars, Skate 3, BioShock, BioShock 2, BioShock Infinite, and Call of Duty: Black Ops.

Hideo Kojima ’Contractually Forbidden’ From Discussing Konami Split

According to a new report from The New Yorker, there is a reason why Metal Gear Solid creator Hideo Kojima did not speak about the terms of his split with Konami when he announced his new studio and game earlier this week. The report claims that Kojima is "contractually forbidden" from discussing the terms of his exit from the Japanese game publisher.

The veteran game designer officially left Konami on December 15 after nearly three decades with Konami. However, a previous report claimed that he actually parted ways with Konami in October. It was believed that he was under a non-compete clause that expired in December.

His new game will be exclusive on console to PlayStation 4, but is also coming to PC. It’s still early days for the project - it doesn’t have a name or a release window, not even a target release window. Kojima’s new studio, Kojima Productions, currently has just four employees and no office.

GameSpot first reported earlier this year that Kojima was likely to leave the company following the completion of Metal Gear Solid V: The Phantom Pain, which was released on September 1. A power struggle between Konami and Kojima Productions, the Kojima-led studio responsible for Metal Gear Solid, resulted in senior staff having limited access to emails, phone calls, and corporate Internet.

In August, a report detailed the troubling corporate culture at Konami. Among other things claimed in the report was that Konami employees are monitored with surveillance cameras while at work.

Kojima first came to work at Konami in 1986. It was there that he created the Metal Gear series, which he has helmed since 1987. His other projects have included Snatcher, Policenauts, Boktai, and Zone of the Enders.

Xbox Live Downed After Threats; Hacker Group Takes Responsibility

A hacker group previously made threats to down the service during Christmas, mimicking a similar high-profile hacker group last year.

Xbox services were downed for a time on Friday following a suspected attack, which a known hacker group claimed to take responsibility for.

Hackers from the Phantom Squad are said to have launched a distributed denial-of-service (DDoS) attack against the Microsoft gaming network.

In a tweet, the group said Xbox maker Microsoft, and rival Sony-owned gaming network PSN, doesn’t "bother working on security" despite their "millions of dollars."

"PSN and Xbox don’t use that money to improve their security. Until they open their eyes, Xbox Live and PSN will remain vulnerable," the group said.

During the attack, the group tweeted: "Xbox Live #Offline," but did not offer any visual proof that they were directly behind the attack.

The group’s account, @PhantomSqaud, was later suspended by Twitter.

As of mid-morning on Friday, Xbox services were back to normal, according to the company’s support pages. Sony’s PSN network is not thought to have been targeted, but a separate tweet by the hacker group warned that it is "next" on their target list.

The first thing you notice after a couple of minutes messing around with Edge besides the option for a cool new dark theme is how smooth

The threats came a week earlier, mirroring the actions almost a year after the infamous Lizard Squad launched a series of network attacks against Xbox Live and Sony’s PSN network. The attacks were so ferocious and long-lasting that new and existing gamers during the Christmas holidays were unable to login for hours or even days at a time, drawing ire from the international gaming community.

The attackers also took down a number of other major sites and networks, including the Dept. of Defense’s global satellite messaging system. A number of the group’s hackers were later arrested by British authorities.

A Microsoft spokesperson did not immediately return a phone call requesting comment.

Hackers Plan To Ruin Christmas Eve for Millions of PlayStation and Xbox Live Gamers

Remember the notorious hacker group Lizard Squad that spoiled last Christmas holidays of many game lovers by knocking the PlayStation Network and Xbox Live offline with apparent Distributed Denial of Service (DDoS) attacks?

But, Will you be able to Play Xbox and PlayStation Game this Christmas?

Probably Not.

Because a new hacking group is threatening to carry out similar attacks by taking down the Xbox LIVE and PlayStation Network for a week during Christmas.

In a series of tweets, a bunch of DDoS hackers calling themselves "Phantom Group" (@PhantomSquad) announced that they will disrupt the XBox Live and PlayStation networks in a coordinated DoS attack.

The attacks could prevent millions of gamers worldwide from enjoying their newly opened Christmas gifts and accessing games online.

Here are the tweets by Phantom Squad:

> We are going to shut down Xbox live and PSN this year on Christmas. And we are going to keep them down for one-week straight #DramaAlert

> Ok, think about this.... Xbox Live and PSN have millions upon millions of dollars... but do they use that money for better security?

> No. PSN and Xbox do not use that money to improve their security... So until they open their eyes, Xbox Live and PSN will remain vulnerable.

A few days ago, Phantom Squad claimed responsibility for knocking Reddit offline, and Reddit confirms that the issue, saying its databases coming "under extreme load" that could have been caused by a DDoS attack.

> "Reddit #Offline Goodnight." Phantom Squad tweeted on December 15, 2015.

Now, the group has turned its crosshairs toward the gaming networks.

However, neither Microsoft nor Sony responsible for managing PlayStation and XBox Live online networks respectively has confirmed the DDoS attacks, but Microsoft, at least, acknowledged issues with Xbox LIVE when Phantom Squad claimed responsibility.

> "Xbox Live #Offline" Phantom Squad tweeted on December 12, 2015.

As a proof, Phantom Squad also posted a video of its cyber attacks.

If the DDoS attack on PSN and XBox is carried out successfully for a week during Christmas, it will again ruin the Christmas holidays for millions of video game lovers worldwide, just like last year.

Since DDoS attacks are so easy to conduct nowadays when there are so many DDoS tools available online, the important point here is whether Microsoft and Sony have upgraded their DDoS defences enough to defend against the attacks.

Hacker Confirms PlayStation 4 Jailbreak!
Exploit Could Open Doors for Pirated Games

Sony's PlayStation 4 the hottest-selling gaming console in the United States has been in the market for a while now, and since its release, hackers have been tinkering with it to find a way to run unauthorized software.

Though breaking the protection on PlayStation 4 is a huge deal, a hacker who calls himself CTurt has claimed to develop a fully jailbroken version of the PlayStation 4 with the help of a kernel exploit that he previously created.

The current jailbreak allows dumping of the system RAM from other processes and installing custom firmware that can be used to run homebrew applications that aren't approved by Sony.

Of course, there is still a few other security issues to get by, but it is a foot in the door for game piracy, which can affect the gaming market as a whole.

The Twitter account of CTurt seems to indicate that currently the exploit only works for PlayStation 4 firmware version 1.76, but apparently it can be tweaked to work for more recent firmware.

CTurt successfully managed to take advantage of an exploit in PlayStation 4 v1.76 to inject an external code in the system, thereby taking control of the hardware.

Sony would certainly be unhappy with the launch of PlayStation 4 jailbreak and would be trying hard to eliminate any vulnerabilities for the most recent version of PS4 firmware.

Man Pleads Guilty to Forcibly Stealing 4.7 Billion Virtual Coins for Use in Online Game RuneScape, Sentenced to 6 Months in Jail

Humza Bajwa pleaded guilty to grand larceny and attempted robbery.

The currency was virtual and the gun was fake but the jail time is real.

A video game obsessive who flashed an imitation pistol to rob a Fordham University student of nearly 5 billion fantasy coins was taken away in cuffs Tuesday to begin six months behind bars.

Humza Bajwa pleaded guilty in Bronx Supreme Court to forcibly stealing 4.7 billion gold coins for use in the role-playing game RuneScape. Gamers use the virtual dough to buy supplies in a medieval online fantasy world.

As part of the plea deal, the Massachusetts native will pay back the $3,300 in real cash he had promised to swap for the gold coins at a July 13, 2012 meeting on the Fordham campus.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

The Real Star Raiders II

Star Raiders was the Atari 8-bit home computer’s killer app, inspiring Ted Nelson to claim that "The Atari machine is the most extraordinary computer graphics box ever made, and Star Raiders is its virtuoso demonstration game." It was not until many years later that a sequel, of sorts, was released. This Star Raiders II was nothing at all like the original, as it was originally The Last Starfighter, a licensed tie-in to that was rebranded to avoid the stench of the box-office flop.

Well now, three decades later, Kevin Savetz of the excellent ANTIC podcast has dropped a bomb on the retrogaming community: there was a real Star Raiders II under construction for a long time, but it disappeared as Atari imploded. Kevin tracked down the author, Aric Wilmunder, and convinced him to release it after all these years. You can download the game for the emulator of your choice, and read the manual and backstory on the Internet Archive.

Commander Keen Turns 25

Commander Keen is an episodic video game developed by id Software in the early 1990s. The series focuses on the adventures of Billy Blaze, an 8-year-old boy who travels through space and assumes the secret identity of "Commander Keen". The series was successful at replicating the side-scrolling action of the Nintendo Entertainment System Super Mario Bros. games in DOS. The cartoon-style platform games are notable for their pioneering use of EGA graphics and shareware distribution, and they were some of the first games by id Software (who went on to later develop Wolfenstein 3D, Doom and Quake). The games were also exciting to the PC gaming community of the time because of John D. Carmack’s smooth-scrolling graphics game engine, which first allowed smooth side scrollers on PC by only redrawing the elements of the screen that actually changed frame to frame.

Today is Commander Keen’s 25th birthday. Keen was one of the very first games I ever played, and everybody I knew at the time was into Keen as well. We swapped floppies around with Keen on them, and I must’ve finished many of the episodes countless times. Commander Keen is part of my childhood, and a landmark in (PC) gaming.

In honour of Keen’s 25th birthday, John Romero published a video

today, in which he shows id Software’s "port" (reverse engineering is probably more accurate) of Super Mario Bros. 3 to the PC. It was created without Nintendo’s consent, and then sent to Nintendo for evaluation. The company had no interest in it, but the knowledge gained would come to use for Keen.

Fascinating.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Twitter Warns Some Users Over Possible Government Hacking

Twitter sent a warning to some users that the social network said may have been targeted by "state-sponsored hackers."

It’s unclear how many people received a letter from Twitter. However, the message warns hackers may be attempting to steal phone numbers, along with email and IP addresses, according to copies of the email shared on Twitter. It was also unknown who the reported hackers are and who they could be working for.

"At this time, we have no evidence they obtained your account information, but we’re actively investigating this matter," a copy of the letter posted online by @Coldhak, a Canadian nonprofit group, said. "We wish we had more we could share, but we don’t have any additional information we can provide at this time."

Among the people who reported receiving the letter were security researchers, activists and journalists.

Twitter did not immediately respond to ABC News’ request for comment.

In October, Facebook said it would begin issuing alerts to users who the social network believes are being targeted by state-sponsored hackers, according to a message posted by Alex Stamos, Facebook’s chief security officer. Google introduced warnings for state-sponsored hacks in 2012.

Red-faced Microsoft Tries to Fix Free Storage Snafu

Too little, too late?

Talk about putting lipstick on a chicken.

Microsoft is trying to make amends for last month s decision to pull its offer of unlimited free OneDrive cloud storage. Clearly, given the negative coverage and customer blowback, this was not one of Microsoft s finest hours. So now, for a limited number of select customers, the company is sort of changing course again, according to this post on the OneDrive customer forum spotted by ComputerWorld.

OneDrive s biggest and most loyal fans can keep their existing 15 gigabytes of free storage after next year when the changes take effect. And if those users also have an additional 15 gigabyte bonus for their photos, they can keep that as well, but they have to sign up here for that privilege.

There are more than 4,200 comments on a Nov. 2 OneDrive user post titled Give us our storage back and more than 7,000 up votes, which gives you an idea of how this change was seen beyond Microsoft HQ.

The whole did we say free? We didn t mean it fiasco shows how tricky it is for tech providers to change course especially if that means taking something that was free or perceived to be free and slapping a price tag on it. And in this case, the freebie was really a perk for existing Microsoft Windows or Office/Office 365 customers who may feel they re paying plenty already to Microsoft.

Under changes announced in November, the company stopped offering free unlimited storage to subscribers paying for Office 365 Home, Personal, or University editions. It announced that move the previous year, claiming that it got rid of storage limits for Office 365 users.

So much for that. Instead those customers would get 1 terabyte of storage with their subscription. Now, 1 terabyte is not nothing, but it s a far cry from unlimited. Or, even 2 terabytes.

In addition, the free OneDrive tier available to anyone shrunk to 5 gigabytes from 15 gigabyte. Office 365 users who wanted to jump ship to some other free- or near-free offer from Google or Dropbox could get a pro-rated discount, according to the Microsoft FAQ.

The rationale for all this unpleasantness was that according to Microsoft some digital hoarders were putting all their CDs, all their photographs, everything onto OneDrive, in what it characterized that as an abuse of the system. But others saw this as a huge company punishing many for the sins of a few.

At least Microsoft, in the form of group program manager Douglas Pearse, appears to get how badly this was handled.

 We realize the announcement came across as blaming customers for using our product. For this, we are truly sorry and would like to apologize to the community, Pearse wrote on the site. Pearse s post also shut down additional comments on the Give us our storage back thread so maybe Microsoft was nearing the end of its own storage allotment? (I kid.)

Microsoft in particular has a problem because it is so big and

profitable, that reversing course on what was called a free perk for paying users of Office 365 looks like a big company trying to save money on the backs of its customers.

Breaking News on EFF Victory: Appeals Court Holds That Email Privacy Protected by Fourth Amendment

In a landmark decision issued today in the criminal appeal of U.S. v. Warshak, the Sixth Circuit Court of Appeals has ruled that the government must have a search warrant before it can secretly seize and search emails stored by email service providers. Closely tracking arguments made by EFF in its amicus brief, the court found that email users have the same reasonable expectation of privacy in their stored email as they do in their phone calls and postal mail.

EFF filed a similar amicus brief with the 6th Circuit in 2006 in a civil suit brought by criminal defendant Warshak against the government for its warrantless seizure of his emails. There, the 6th Circuit agreed with EFF that email users have a Fourth Amendment-protected expectation of privacy in the email they store with their email providers, though that decision was later vacated on procedural grounds. Warshak's appeal of his criminal conviction has brought the issue back to the Sixth Circuit, and once again the court has agreed with EFF and held that email users have a Fourth Amendment-protected reasonable expectation of privacy in the contents of their email accounts.

As the Court held today,

> Given the fundamental similarities between email and traditional forms of communication [like postal mail and telephone calls], it would defy common sense to afford emails lesser Fourth Amendment protection.... It follows that email requires strong protection under the Fourth Amendment; otherwise the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.... [T]he police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call - unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement....

Today's decision is the only federal appellate decision currently on the books that squarely rules on this critically important privacy issue, an issue made all the more important by the fact that current federal law--in particular, the Stored Communications Act - allows the government to secretly obtain emails without a warrant in many situations. We hope that this ruling will spur Congress to update that law as EFF and its partners in the Digital Due Process coalition have urged, so that when the government secretly demands someone's email without probable cause, the email provider can confidently say: "Come back with a warrant."

Anonymous Knockoff Donald Trump Website Against Anti-Muslim Speech

Remember a couple of months ago a hacker defaced Donald Trump s official website with a tribute message for Jon Stewart? Now Anonymous has done the same but with a DDoS attack.

The online hacktivist group Anonymous has conducted a powerful DDoS attack on one of the Donald trump s website for Trump Tower New York trumptowerny.com and forced it to stay offline.

The group says the reason for targeting Trump s website was due to his anti-Muslim hate speech a couple of days ago.

Earlier the hacktivist organization had announced the attack on the Republican presidential candidate and it didn t take long for them to carry out DDoS attacks on the candidate s site.

Right after the attack the group posted a video, leaving this message for Trump:

> It has come to our attention that you want to ban all Muslims to enter the United States. This policy is going to have a huge impact. This is what ISIS wants.

The Trump Tower New York s website is protected by CloudFlare. The site was available online in cache version for a while, however, it s been more than 12 hours and the site is still down.

It seems Anonymous is on a role at the moment. The other day the group targeted Japanese Prime Minister s site and have already declared war against ISIS with the trolling day on 11th December. So, it would be interesting to see how the Anonymous carries out both these operations.

In February 2013, Trump s Twitter account was hacked and whoever was behind the attack tweeted a quote from Lil Wayne s song These hoes think they classy, well that s the class I m skippen.

Target Back on Naughty List With Another Security Vulnerability

Hackers can access your personal information from Target - again - thanks to a flaw in the retailer’s mobile app.

In a blog post Tuesday, researchers from security company Avast revealed the flaw, which allows unauthorized access to customers’ addresses, phone numbers and other personal information from wish lists created with the Target app. The only merry tidings are that credit card numbers don’t appear to be stored with the wish lists, so financial information isn’t vulnerable.

If this sounds familiar, it’s because last year we learned that hackers breached Target’s systems and stole the credit card

information of up to 70 million customers. Though hackers have the opportunity to steal the wish list information right now, Avast researchers have found only that it would be possible. It’s unknown whether the security hole has been exploited.

The wish list information was still vulnerable to hacking as of Tuesday afternoon, according to an Avast representative who added that the company hadn’t notified Target of the problem. The representative didn’t immediately respond to a follow-up question about why Avast hadn’t informed the retailer of the flaw.

Target disabled elements of its wish list app Tuesday evening after being informed of the vulnerability, said a spokeswoman for the Minneapolis, Minnesota-based retailer.

"We apologize for any challenges guests may be facing while trying to access their registry," Molly Snyder, a communications manager at Target, said in a statement. "Our teams are working diligently overnight to resume full functionality."

Avast said Tuesday it discovered the flaw while examining the security and privacy levels of various mobile buying apps. During their examination, researchers looked at what permissions were granted users, in addition to trying to hack the apps.

As if shopping on mobile phones wasn’t vexing enough, the discovery shows that some major shopping apps don’t have security or privacy nailed down.

On the privacy side, researchers at Avast singled out the Walgreens shopping app for requesting user permissions that had nothing to do with the app’s purpose. That means it could be collecting information you never meant to share with your friendly neighborhood drugstore.

Walgreens spokeswoman Mailee Garcia said the permissions cited by Avast were in fact related to the app’s purpose.

"For example, these include our Refill by Scan feature, which requires a smartphone camera; telehealth services and consultations, which require a microphone... and connection of personal fitness devices, which require Bluetooth," Garcia said. "Any suggestion that our app’s permissions are unrelated to its purpose are inaccurate."

However, Avast researchers said this level of permissions wasn’t half bad.

"In fact, compared to other apps out there they are decent," wrote Avast researcher Filip Chytry.

Well, fa la la la la.

U.K. Police Arrest Man in Connection With VTech Hacking

U.K. police on Tuesday arrested a 21-year-old man as part of an investigation into the late November hacking of Hong Kong-based

digital-learning toy maker VTech Holdings Ltd , a cyber-attack that garnered global attention as the personal data of 6.4 million children worldwide were exposed.

Officers from the South East Regional Organized Crime Unit arrested the man in Bracknell, about 30 miles west of London, on suspicions of unauthorized access to a computer to facilitate the commission of an offense, the police said.

The man wasn t named and no further details were provided.

You Can Hack Into A Linux Computer Just by Pressing 'Backspace' 28 Times

So what would anyone need to bypass password protection on your computer?

It just needs to hit the backspace key 28 times, for at least the computer running Linux operating system.

Wait, what?

A pair of security researchers from the University of Valencia have uncovered a bizarre bug in several distributions of Linux that could allow anyone to bypass any kind of authentication during boot-up just by pressing backspace key 28 times.

This time, the issue is neither in a kernel nor in an operating system itself, but rather the vulnerability actually resides in Grub2, the popular Grand Unified Bootloader, which is used by most Linux systems to boot the operating system when the PC starts.

The source of the vulnerability is nothing but an integer underflow fault that was introduced with single commit in Grub version 1.98 (December 2009) b391bdb2f2c5ccf29da66cecdbfb7566656a704d affecting the grub_password_get() function.

If your computer system is vulnerable to this bug:

Just hit the backspace key 28 times at the Grub username prompt during power-up. This will open a "Grub rescue shell" under Grub2 versions 1.98 to version 2.02.

This rescue shell allows unauthenticated access to a computer and the ability to load another environment.

From this shell, an attacker could gain access to all the data on your computer, and can misuse it to steal or delete all the data, or install persistent malware or rootkit, according to researchers Ismael Ripoll and Hector Marco, who published their research on Tuesday.

The Grub vulnerability affects Linux systems from December 2009 to the present date, though older Linux systems may also be affected.

The good news is the researchers have made an emergency patch to fix the Grub2 vulnerability. So if you are a Linux user and worried your system might be vulnerable, you can apply this emergency patch, available here.

Meanwhile, many major distributions, including Ubuntu, Red Hat, and Debian have also released emergency patches to fix the issue.

Linux is often thought to be a super secure operating system compare to others, and this Grub vulnerability could be a good reminder that it’s high time to take physical security just as seriously as network security.

Facebook Sanitizes Your Year, Scrubbing Out The Bad Stuff

Facebook rolled out a personalized Year in Review page for its users that attempts to remember only the good times.

Launched on Wednesday, the page displays many of the photos you’ve posted on Facebook throughout 2015, offering you a visual tour of your entire year, at least as you shared it on the site. Rather than show you all of your photos, the social network applied some technical smarts by automatically eliminating photos associated with negative events, such as a death in the family.

You can edit your photo lineup to add photos the site missed or remove ones you’d rather not see again. You can select up to 10 photos altogether.

Social networks like Facebook offer an outlet to share both the good and bad times of your life, as you see fit. They also routinely try to present what they think you want to see. In the case of Facebook, the world’s largest social network, that includes the "top stories" in your feed, reminders to wish friends a happy birthday and memories you can share of an individual posts you made years ago. It’s all about getting you to visit Facebook more often and to linger longer when you do.

But not every memory on Facebook is a good one.

In 2014, Facebook triggered criticism when the photo of a girl who died appeared on the Year in Review page of her father. The photo was surrounded by images of people dancing and partying as if it were a happy event, prompting the father to compose a blog post expressing the pain and grief he experienced as a result. The Menlo Park, California, company wanted to avoid the same type of situation this year, thus trying to better control your photo results.

"We heard feedback last year that we need to do more to select the photos that are most enjoyable to people and make it easier for them to edit the photos they see and share in their Year in Review," a Facebook spokesperson said. "So we’ve applied a unique set of filters to Your Year in Review to reduce the chance we’ll show you a photo you don’t want to see. And for the photos that our algorithms don’t catch, we’re giving people control over the photos in their Year in Review."

The photos you first see in your Year in Review page use filters that Facebook applies to other features, such as On This Day, which looks back on a specific day in your Facebook history, a company spokesman said. You won't see photos where memorialized accounts or ex-spouses are tagged, or photos with people you've blocked. You can add such photos manually if you wish.

"We know that people share a range of content on Facebook, and we want them to be able to create a Year in Review that accurately depicts their year, no matter what kind of memories they want to highlight," the spokesman added.

You can view your own Year in Review through your Facebook News Feed or catch it via a dedicated page. You can also share your Year in Review with your Facebook friends so they can watch the journey life took you on throughout the year.

N3XT Advanced CHIP That Could Make Your Computer 1000 Times Faster

Researchers have come up with an all new way to revolutionize the standard computer chip that comes inbuilt in all our electronics.

Researchers from Carnegie Mellon, Stanford, and the University of California, Berkeley among others, have invented a new material that could replace the 'silicon' in conventional chips built in all electronic devices making the device's processing speed 1,000 times faster.

This means that the new chip made with nano-material could solve complex problems in a fraction of the time our computers take.

The brand new chip, dubbed Nano-Engineered Computing Systems Technology (N3XT), takes the landscape from a resource-heavy single-storey layout to an efficient 'Skyscraper' approach, claims a Rebooting Computing special issue of the IEEE Computer journal.

The standard silicon chips currently used in all electronic devices have one major issue:

The silicon chips are arranged like standalone houses in the suburbs.

This means these chips are single-storeys in which each "house" in the neighbourhood are connected with wires that carry digital data.

The drawback of silicon chips is that the data in these chips travels longer distances and wastes energy, often causing digital traffic jams while processing.

N3XT chips that are made from carbon nanotube transistors are tiny cylindrical molecules of carbon that efficiently conduct heat and electricity.

The N3XT model splits processors and memory into, say, different

’floors’ in a skyscraper.

All those floors are then connected by millions of tiny electronic elevators, called ’vias,’ that are used to transport data between chips.

The big advantage of Skyscraper approach data moves much faster, and more efficiently over shorter distances (vertically) than across a larger area (horizontally) like in current silicon chips.

"When you combine higher speed with lower energy use, N3XT systems outperform conventional approaches by a factor of a thousand," said H. -S. Philip Wong, the Professor, who authored the paper.

Another advantage of Skyscraper chips over Silicon chips is that:

Silicon chip cannot be piled on top of each other like in N3XT chip, because, during fabrication silicon chip gets extremely hot (almost 1,000 degrees centigrade) that ends up damaging the layers below.

Whereas the N3XT chip can be fabricated at much lower temperatures than silicon chip, so it can easily be layered without damaging the stacks below.

It sounds like an entirely different approach to computer memory and, of course, this kind of computing knowledge is new to me. But, it’s interesting to know that the approach could bring a macro-level revolution in chip architecture that took place more than a century ago.

Teens Are Using Secret Hashtags To Share Dangerous Habits

Rule-breaking may be just as irresistible to teenagers today as it was in their parents day, but a new study of secret social media hashtags like #selfharmmm suggests that new technology is helping kids share dangerous behaviors more easily than ever before.

When it comes to what s known as non-suicidal self-injury cutting, burning and scratching done with damage rather than death in mind teens can be quite crafty at deploying hashtags that mask their activities, evade content safeguards and advisory warnings, and make it much harder for parents to monitor their virtual lives.

The online communities that develop around these hashtags can draw in adolescents and provide them a strong sense of belonging and support that is centered on these unhealthy behaviors, said lead study author Dr. Megan Moreno, a specialist in adolescent medicine at the University of Washington and Seattle Children s Research Institute.

This can make recovery from these behaviors more challenging, Moreno added by email.

Moreno and colleagues used the search term #selfharmmm to identify public posts on the social media platform Instagram, a photo-sharing service popular with teens, that related to destructive habits like cutting and burning.

Then, they used the search results to identify a list of ambiguous hashtags such as #blithe, #MySecretFamily and #SecretSociety123 that were tied to the same dangerous behaviors.

Other hashtags related to mental health conditions through use of common names, such as #Deb for depression, #Annie for anxiety, and #Olive for obsessive-compulsive disorder.

The number of search results for self-harm hashtags was high and grew over time.

The broad term #cat, which refers to cutting, had more than 44 million search results in 2014 and more than 56 million in 2015, the study team reports in the Journal of Adolescent Health.

Over that same period, use of #selfharmmm also grew, generating 1.7 million search results in 2014 and more than 2.4 million in 2015. In its various permutations, #SecretSociety123 grew by approximately 500,000 search results.

One limitation of the study, the authors acknowledge, is its reliance on data generated by starting with a single term, #selfharmmm, which was selected for its popularity as a portal into online communities that focus on these behaviors but might omit some relevant content. The study results are also limited to self-harm, and don t look at other destructive behaviors such as substance abuse or eating disorders.

Still, the results show that parents can t rely on social media sites to provide safe places for their kids, and highlight the need for parents to be proactive in communicating with children about their online experiences, Moreno said.

One effective response to unhealthy content on social media may involve meeting teens where they live their virtual lives, suggests a second study focused on eating disorders like anorexia and bulimia.

For this study, researchers analyzed videos posted on YouTube that promoted eating disorders using terms like pro-ana as well as posts opposed to the dangerous behavior with terms like anti pro-ana.

While pro-ana videos were more popular, garnering 4.8 million views compared to just 1.4 million views for clips opposed to this behavior, the opposition content drew more comments overall and more positive feedback, the study found.

This suggests that posting content advocating against dangerous behavior might help combat social media content promoting unhealthy choices, said lead study author Dr. Atte Oksanen of the University of Tampere in Finland.

 YouTube has this powerful user community opposing pro-anorexia users, Oksanen said by email. Kids might not listen to their

parents or adults in general, but they still might be influenced by their peers within social media and user communities might succeed where parents and health campaigns fail.

Facebook Is Relaxing Its Real-name Policy

Until now, you had to use your "authentic" name on Facebook. That’s no longer the case.

The world’s largest social network said it is relaxing its rules for how people identify themselves, allowing them to more easily use the name "people know them by." In addition, the service said it would make it harder for harassers to ask Facebook to disable users’ accounts.

"We recognize that it’s also important that this policy works for everyone, especially for communities who are marginalized or face discrimination," two Facebook employees wrote in a blog post announcing the moves Tuesday.

Facebook said it has changed its systems to be more forgiving about uncommon names, hoping to reduce the number of people who have to verify with Facebook who they are. The company also said it will allow users to verify their information with a wider variety of documents beyond typical governmental IDs. They will also be able to explain why they aren’t using their legal name, if Facebook asks. "This additional information will help our review teams better understand the situation so they can provide more personalized support," the company said.

The move will be particularly welcome by the lesbian, gay, bisexual and transgender communities, which have criticized Facebook for its rigid rules requiring users to identify themselves by their real names. The company, which counts more than 1.5 billion people using its service each month, has defended the rule, saying that when people are forced to use their real name on the Internet it adds weight and authenticity to what they’re saying. Other, smaller, social networks like Twitter and Reddit don’t require users to identify themselves with their real names.

The debate hit a tipping point last year, when gay rights activists said their Facebook accounts were being deactivated, seemingly as a result of a coordinated campaign by detractors who reported them under Facebook’s naming policies.

Groups like the Sisters of Perpetual Indulgence in San Francisco, who mostly dress in drag and go by stage names, began protesting Facebook’s rules. The group said Facebook wasn’t being fair to domestic violence sufferers, transgender people and political refugees, many of whom often use pseudonyms online to protect themselves from people who might harm them in the real world.

"All people should feel safe using their preferred identity when speaking, online or off," the group wrote in a letter to Facebook last year.

Now, Facebook said people who report "fake names" will have to explain what’s wrong, including why their name on Facebook is "different from everyday life."

The new tools will first be tested in the US, Facebook said, but will make them more widely available as they’re refined.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.